ZENworks®
Endpoint Security Management v3.5

Release Notes

August 3, 2007

Copyright © 2007 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher. Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell

Contents

Section 1 - Overview 3
1.1 Document Purpose 3
1.2 Background 3
1.3 Documentation 3
Section 2 - Installation and Licensing 3
2.1 Installation and Licensing 3
Section 3 - New Features in this Release 4
3.1 Storage Encryption Solution 4
Section 4 - Known Issues/Limitations 5
4.1 Installation 5
4.2 Upgrades 5
4.3 Directory Service 5
4.4 Management Console 5
4.5 Application Blocking 6
4.6 Client Self Defense 6
4.7 Communications Hardware Control 6
4.8 Custom User Messages 6
4.9 Data Encryption 7
4.10 Endpoint Integrity 7
4.11 Firewall 7
4.12 Network Environments 7
4.13 Storage Device Control 7
4.14 VPN Enforcement 7
4.15 Wi-Fi™ Connectivity Control 8

Copyright © 2007 Novell, Inc. All rights reserved.

Section 1 - Overview

1.1 Document Purpose

The purpose of this document is to detail the new features and known issues for Novell® ZENworks® Endpoint Security Management (ESM) version 3.5. This document supports **ESM 3.5.019**, and subsequent releases.

1.2 Background

ZENworks ESM 3.5 is the latest in endpoint security. This version now includes new capabilities for file and folder encryption requiring authorization prior to viewing stored data. ESM 3.5 also includes Wi-Fi control, application control, personal firewall, and anti-virus and anti-malware policy control. The system easily manages encryption keys throughout the enterprise via the distributed security policy, making data protection enforcement transparent to the end-users and easy for administrators.

1.3 Documentation

Product documentation is available in the ESM 3.5 installation package.
The available ESM manuals for this release are:

- ZENworks ESM Installation and Quick-Start Guide
- ZENworks ESM Administrator's Manual
- ZENworks Security Client User's Manual

Documentation for ESM 3.5 is available in PDF format. To view, use Adobe Acrobat Reader. Acrobat Reader is available free at: http://www.adobe.com/products/acrobat/readstep2.html.

Section 2 - Installation and Licensing

2.1 Installation and Licensing

The ZENworks ESM Installation and Quick-start Guide is included with the ESM documentation. Guidelines for requirements and installation procedures are included.

Licenses are sent separately and should be installed as described in the 3.5-license.pdf document, which is sent with the license.

Copyright © 2007 Novell, Inc. All rights reserved.

Section 3 - New Features in this Release

3.1 Storage Encryption Solution

Storage Encryption Solution provides complete, centralized security management of all mobile data by actively enforcing a corporate encryption policy on the endpoint itself.

- Centrally create, distribute, enforce, and audit encryption policies on all endpoints and removable storage devices
- Encrypt all files saved to, or copied to, a specific directory on all fixed disk partitions
- Encrypt all files copied to removable storage devices
- Share files freely within an organization while blocking unauthorized access to files
- Share password-protected, encrypted files with people outside the organization through an available decryption utility
- Easily update, backup, and recover keys via policy without losing data

Data encryption is enforced through the creation and distribution of data encryption security policies. Sensitive data on the endpoint can be stored in a safe, encrypted folder. The end-user can access and copy this data outside of the encrypted folder and share the files, however while in that folder, the data will remain encrypted. Attempts to read the data by anyone who is not an authorized user for that machine will be unsuccessful. When the policy is activated, an encrypted "Safe Harbor" folder will be added to the root directory of all fixed-disk drives on the endpoint.

Sensitive data placed on a thumbdrive or other removable media device will be immediately encrypted, and can only be read on the machines in the same policy group. A sharing folder can optionally be activated, which will allow the user to share the files with persons outside their policy group via a password

Copyright © 2007 Novell, Inc. All rights reserved.

Section 4 - Known Issues/Limitations

4.1 Installation

- ESM 3.5 does not run on Windows XP 64-bit Operating Systems. We do support 64-bit CPU on a 32-bit OS. We do not currently support Microsoft Vista.
- ESM 3.5 is not localized for languages other than US English.
- ESM 3.5 Servers and Stand-Alone Management Console will not install using SQL Server Express 2005.

4.2 Upgrades

- Contact your Support representative for assistance with any upgrade.
- Back-up all SQL databases and the Novell Setup Files folder, and export all security policies prior to upgrading.
- Managed (back-end servers) upgrade does not check to see if the database has active connections. Users must make sure that the SQL databases are not in use before starting an upgrade.
- The 3.1 Policy Editor cannot be run against a 3.5 Management Server installation.
- Upgrading an existing 3.2 policy to a 3.5 policy will lose password override. When a 3.2 policy has a password override it must be re-entered in the 3.5 policy before it is published. This is by design.

4.3 Directory Service

In some Active Directory multiple domain configurations running Windows NT 4 compatibility (mixed mode used during NT4 to Active Directory migration), the child Domain Users and Domain Computers may be captured during user registration and be shown erroneously within the Management Console. If you change the child domains to Active Directory Native mode, this issue will not be observed.

4.4 Management Console

- Clicking on an error message in the Management Console may not always take you to the correct screen. This limitation manifests itself on screens with multiple tabs.
- Removing Management Console permissions from a user does not take effect until the user's Management Console session is terminated.

Copyright © 2007 Novell, Inc. All rights reserved.

4.5 Application Blocking

- Blocking an application from execution will not shut down an application that is actively open on the endpoint.
- Blocking network access to an application will not stop access to an application that is actively streaming network data on the endpoint.
- Blocking network access to an application will not stop access to an application that is getting data from a Network Share.
- Applications blocked for execution will still launch if they are started from a network drive share that has “system” blocked from read access.
- Network Application Control does not function if the device is booted to Safe Mode with Networking.

4.6 Client Self Defense

For full client self defense to be in effect, an uninstall password must be implemented.

4.7 Communications Hardware Control

- In 3.5, MOST Widcom-based Bluetooth® solutions are also supported. Specifically, supported devices include:
    - Devices using the Microsoft standard Type GUID {e0cbf06cL-cd8b-4647-bb8a263b43f0f974}
    - Devices using the Dell USB Bluetooth module; the Dell Type GUID {7240100F-6512-4548-8418-9EBB5C6A1A94}
    - HP/Compaq Bluetooth Module; the HP Type GUID {95C7A0A0L-3094-11D7-A202-00508B9D7D5A}

To determine if a device is supported, follow these steps:

1. Open Regedit
2. Navigate to “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class”
3. Search for the listed type GUID Keys (listed above). Note: the Microsoft key must have more than one subkey to be valid.

4.8 Custom User Messages

Disable Wi-Fi transmissions and Disable Adapter Bridging messages are only shown if the end user tries to bypass the enforcement. They will be enforced without a warning message.

Copyright © 2007 Novell, Inc. All rights reserved.

4.9 Data Encryption

- SES is only supported on Windows XP SP2 because of required Filter Manager support. ESM 3.5 will install on Windows 2000 SP4 and XP SP1, but when those operating systems receive an encryption policy, the encryption requests will be ignored and an alert sent to the administrator.

- This version of ESM 3.5 does not permit a policy to enable Hardware Device Control and Encryption of Removable Media at the same time.

4.10 Endpoint Integrity

- Some of ESM's pre-installed antivirus and spyware rules may need to me modified for a specific or custom-installed version of the antivirus or spyware software.

4.11 Firewall

- In most modes, the ZENworks firewall does not allow incoming connections to dynamically assigned ports. If an application requires an incoming connection to be allowed; the port must be static and a firewall setting of "Open" created to allow the incoming connection. If the incoming connection is from a known remote device an ACL can be used.

- The default "All Adaptive" (Stateful) firewall setting will not allow an active FTP session; use passive FTP instead. A good reference to explain active versus passive FTP is http://slacksite.com/other/ftp.html.

4.12 Network Environments

Adapter-Specific Network Environments that become invalid can cause the client to continue to switch between the location the environment is assigned to, and Unknown. To prevent this, set the adapter type of the network environment to an adapter that is enabled at the location.

4.13 Storage Device Control

- Not all USB disk-drives have serial numbers, some have them "made up" (depending on the port and drive combination) and some are not unique. Most thumb drives have what appears to be a unique serial number.

- If a CD/DVD burning device is added AFTER the SSC is installed, policies specifying "Read Only" to that device will NOT be enforced if using 3rd party burning software such as Roxio, or Nero.

4.14 VPN Enforcement

- VPN Enforcement in its most secure implementation requires an All Closed firewall setting, with applicable ACLs to the VPN Concentrator's appropriate communication ports, and the VPN set up to be FULL TUNNEL (not Split Tunnel).

Copyright © 2007 Novell, Inc. All rights reserved.

4.15 Wi-Fi™ Connectivity Control

- WPA Access Points can be identified for Filtering (we do not differentiate between WPA and WPA2). ESM 3.5 only distributes WEP keys.

- Certain outdated wireless adapters will not function correctly when managed by ZENworks. These include:
    - Orinoco 8470-WD Gold
    - 3Com 3CRWE62092B
    - Dell True Mobile 1180
    - Proxim Orinoco 802.11bg combo card

Copyright © 2007 Novell, Inc. All rights reserved.